*** When this bulletin was released, it incorrectly stated that it was for the week of May 15. The vulnerabilities referenced below were actually recorded during the week of May 8.**

Please note that US-CERT has changed the look and scope of the Cyber Security Bulletin.

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
180solutions -- Zango	180solutions Zango downloads "required Adware components" without checking integrity or authenticity, which might allow context-dependent attackers to execute arbitrary code by subverting the DNS resolution of static.zangocash.com.	2006-01-02 2006-05-11	10.0	CVE-2006-2324 BUGTRAQ OTHER-REF
ACal -- ACal	PHP remote file inclusion vulnerability in day.php in ACal 2.2.6 allows remote attackers to execute arbitrary PHP code via a URL in the path parameter.	unknown 2006-05-09	7.0	CVE-2006-2261 OTHER-REF BID FRSIRT SECUNIA
Adobe -- Dreamweaver MX Adobe -- Dreamweaver	Adobe Dreamweaver 8 before 8.0.2 and MX 2004 can generate code that allows SQL injection attacks in the (1) ColdFusion, (2) PHP mySQL, (3) ASP, (4) ASP.NET, and (5) JSP server models.	unknown 2006-05-09	7.0	CVE-2006-2042 ADOBE
Arabless -- SaphpLesson	Multiple SQL injection vulnerabilities in SaphpLesson 3.0 allow remote attackers to execute arbitrary SQL commands via (1) the Find parameter in (a) search.php, and the (2) LID and (3) Rate parameters in (b) misc.php.	2006-04-29 2006-05-09	7.0	CVE-2006-2279 BUGTRAQ FRSIRT SECUNIA
Chirpy! -- Chirpy!	SQL injection vulnerability in Chirpy! 0.1 allows remote attackers to execute arbitrary SQL commands via unspecified parameters.	unknown 2006-05-09	7.0	CVE-2006-2266 NEOHAPSIS OSVDB
Cisco -- PIX Firewall Cisco -- FWSM Cisco -- PIX/ASA	Cisco PIX 7.0.x before 7.0.x and 6.3.x before 6.3.5(112), and FWSM 2.3.x and 3.x, when used with Websense 5.5.2, allows remote attackers to bypass HTTP access restrictions by splitting an HTTP request into multiple packets, which prevents the request from being sent to Websense for inspection.	2005-11-04 2006-05-09	7.0	CVE-2006-0515 BUGTRAQ OTHER-REF BID
Cisco -- Secure ACS for Windows NT Cisco -- Secure ACS for Windows Server	Cisco Secure Access Control Server (ACS) 3.x for Windows stores ACS administrator passwords and the master key in the registry with insecure permissions, which allows local users and remote administrators to decrypt the passwords by using Microsoft's cryptographic API functions to obtain the plaintext version of the master key.	2006-05-08 2006-05-09	7.0	CVE-2006-0561 BUGTRAQ BUGTRAQ SYMANTEC CISCO BID FRSIRT SECTRACK
Claroline -- Claroline Dokeos -- Dokeos	Multiple PHP remote file inclusion vulnerabilities in Claroline 1.7.5 allow remote attackers to execute arbitrary PHP code via a URL in the (1) clarolineRepositorySys parameter in ldap.inc.php and the (2) claro_CasLibPath parameter in casProcess.inc.php.	unknown 2006-05-09	7.0	CVE-2006-2284 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
Creative Software -- Community Portal	Multiple SQL injection vulnerabilities in Creative Community Portal 1.1 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) article_id parameter to (a) ArticleView.php, (2) forum_id parameter to (b) DiscView.php or (c) Discussions.php, (3) event_id parameter to (d) EventView.php, (4) AddVote and (5) answer_id parameter to (e)	unknown 2006-05-09	7.0	CVE-2006-2255 OTHER-REF FRSIRT SECUNIA BID

	PollResults.php, or (7) mid parameter to (f) DiscReply.php.			
Dokeos -- Dokeos community release Dokeos -- Dokeos	Multiple PHP remote file inclusion vulnerabilities in claro_init_global.inc.php in Dokeos 1.6.3 and earlier, and Dokeos community release 2.0.3, allow remote attackers to execute arbitrary PHP code via a URL in the (1) rootSys and (2) clarolineRepositorySys parameters, and possibly the (3) lang_path, (4) extAuthSource, (5) thisAuthSource, (6) main_configuration_file_path, (7) phpDigIncCn, and (8) drs parameters.	unknown 2006-05-09	7.0	CVE-2006-2286 OTHER-REF OTHER-REF
DUware -- DUgallery	SQL injection vulnerability in admin_default.asp in DUGallery 2.x allows remote attackers to execute arbitrary SQL commands via the (1) Login or (2) password field.	unknown 2006-05-11	7.0	CVE-2006-2302 BUGTRAQ BID
FlexCustomer -- FlexCustomer	SQL injection vulnerability in FlexCustomer 0.0.4 and earlier allows remote attackers to bypass authentication and execute arbitrary SQL commands via the admin and ordinary user interface, probably involving the (1) checkuser and (2) checkpass parameters to (a) admin/index.php, and (3) username and (4) password parameters to (b) index.php.	unknown 2006-05-09	7.0	CVE-2006-2268 BUGTRAQ BID FRSIRT SECUNIA
id software -- Quake 3 engine	Directory traversal vulnerability in Quake 3 engine, as used in products including Quake3 Arena, Return to Castle Wolfenstein, Wolfenstein: Enemy Territory, and Star Trek Voyager: Elite Force, when the sv_allowdownload cvar is enabled, allows remote attackers to read arbitrary files from the server via ".." sequences in a .pk3 file request.	unknown 2006-05-09	7.0	CVE-2006-2082 BUGTRAQ BID
id Software -- Quake 3 Engine id Software -- Return to Castle Wolfenstein id Software -- Quake 3 Arena id Software -- Wolfenstein: Enemy Territory	Buffer overflow in the Quake 3 Engine, as used by (1) ET 2.60, (2) Return to Castle Wolfenstein 1.41, and (3) Quake III Arena 1.32b allows remote attackers to execute arbitrary commands via a long remapShader command.	unknown 2006-05-08	8.0	CVE-2006-2236 OTHER-REF BID FRSIRT SECUNIA BUGTRAQ OSVDB XF
Ideal Science -- IdealBB	Multiple SQL injection vulnerabilities in Ideal Science Ideal BB 1.5.4a and earlier allow remote attackers to execute arbitrary SQL commands via multiple unspecified vectors related to stored procedure calls. NOTE: due to lack of details from the researcher, it is not clear whether this overlaps CVE-2004-2209.	unknown 2006-05-11	7.0	CVE-2006-2320 BUGTRAQ OTHER-REF BID
ISPConfig -- ISPConfig	PHP remote file inclusion vulnerability in session.inc.php in ISPConfig 2.2.2 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the go_info[server][classes_root] parameter.	unknown 2006-05-11	7.0	CVE-2006-2315 OTHER-REF BID FRSIRT SECUNIA
Jetbox -- Jetbox CMS	PHP remote file inclusion vulnerability in includes/config.php in Jetbox CMS 2.1 allows remote attackers to execute arbitrary code via a URL in the relative_script_path parameter.	unknown 2006-05-09	7.0	CVE-2006-2270 BUGTRAQ BID FRSIRT SECUNIA
Keyvan1 -- EImagePro	Multiple SQL injection vulnerabilities in EImagePro allow remote attackers to execute arbitrary SQL commands via the (1) CatID parameter to subList.asp, (2) SubjectID parameter to imageList.asp, or (3) Pic parameter to view.asp.	unknown 2006-05-11	7.0	CVE-2006-2300 OTHER-REF BID FRSIRT SECUNIA
MaxxCode -- MaxxSchedule	SQL injection vulnerability in Logon.asp in MaxxSchedule 1.0 allows remote attackers to execute arbitrary SQL commands via the txtLogon parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-05-09	7.0	CVE-2006-2259 BID FRSIRT SECUNIA
Microsoft -- Exchange Server	Unspecified vulnerability in Microsoft Exchange allows remote attackers to execute arbitrary code via e-mail messages with crafted (1) vCal or (2) iCal Calendar properties.	unknown 2006-05-09	7.0	CVE-2006-0027 MS CERT CERT-VN
Microsoft -- Windows NT Microsoft -- Windows 2000 Microsoft -- Windows Server 2003 Microsoft -- Microsoft Distributed Transaction Coordinator Microsoft -- Windows XP	Heap-based buffer overflow in the CRpcIoManagerServer::BuildContext function in msdtcprx.dll for Microsoft Distributed Transaction Coordinator (MSDTC) for Windows NT 4.0 and Windows 2000 SP2 and SP3 allows remote attackers to execute arbitrary code via a long fifth argument to the BuildContextW or BuildContext opcode, aka the MSDTC Invalid Memory Access Vulnerability.	2005-10-11 2006-05-09	7.0	CVE-2006-0034 BUGTRAQ OTHER-REF MS BID FRSIRT SECUNIA
OnlyScript.info -- Online Universal Payment System Script	Cross-site scripting (XSS) vulnerability in index.php in OnlyScript.info Online Universal Payment System Script allows remote attackers to inject arbitrary web script or HTML via the read parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. Also, this issue might be resultant from directory traversal.	unknown 2006-05-11	7.0	CVE-2006-2325 BID FRSIRT SECUNIA

Otterware -- Statit	PHP remote file inclusion vulnerability in visible_count_inc.php in Statit 4 (060207) allows remote attackers to execute arbitrary PHP code via a URL in the statitpath parameter.	unknown 2006-05-09	7.0	CVE-2006-2253 OTHER-REF FRSIRT SECUNIA BID
OzzyWork -- Galeri	SQL injection vulnerability in admin_default.asp in OzzyWork Galeri allows remote attackers to execute arbitrary SQL commands via the (1) Login or (2) password fields.	unknown 2006-05-11	7.0	CVE-2006-2301 BUGTRAQ BID
PlaNet Concept -- plaNetStat	PlaNet Concept plaNetStat 20050127 allows remote attackers to gain administrative privileges, and view and configure log files, via a direct request to the (1) admin.php or (2) settings.php page.	2006-05-09 2006-05-11	7.0	CVE-2006-2338 BUGTRAQ
Sophos -- Anti-Virus for Windows 5.x Sophos -- Anti-Virus for Windows 4.x	Multiple Sophos Anti-Virus products, including Anti-Virus for Windows 5.x before 5.2.1 and 4.x before 4.05, when cabinet file inspection is enabled, allows remote attackers to execute arbitrary code via a CAB file with "invalid folder count values," which leads to heap corruption.	unknown 2006-05-10	7.0	CVE-2006-0994 BUGTRAQ OTHER-REF BID FRSIRT SECTRACK SECUNIA
SpiffyJr -- phpRaid	Multiple PHP remote file inclusion vulnerabilities in SpiffyJr phpRaid 2.9.5 through 3.0.b3 allow remote attackers to execute arbitrary PHP code via a URL in the phpbb_root_path parameter in (1) auth.php and (2) auth_phpbb when the phpBB portal is enabled, and via a URL in the smf_root_path parameter in (3) auth.php and (4) auth_SMF when the SMF portal is enabled.	unknown 2006-05-09	7.0	CVE-2006-2283 BUGTRAQ BUGTRAQ BID
timobraun -- Dynamic Galerie	Cross-site scripting (XSS) vulnerability in Dynamic Galerie 1.0 allows remote attackers to inject arbitrary web script or HTML via the pfad parameter in (1) index.php and (2) galerie.php. NOTE: this issue might be resultant from directory traversal.	unknown 2006-05-09	7.0	CVE-2006-2294 OTHER-REF BID FRSIRT SECUNIA
timobraun -- Dynamic Galerie	Directory traversal vulnerability in Dynamic Galerie 1.0 allows remote attackers to access arbitrary files via an absolute path in the pfad parameter to (1) index.php and (2) galerie.php.	unknown 2006-05-09	7.0	CVE-2006-2295 OTHER-REF BID FRSIRT SECUNIA
Virtual Programming -- VP-ASP	SQL injection vulnerability in shopcurrency.asp in VP-ASP 6.00 allows remote attackers to execute arbitrary SQL commands via the cid parameter.	unknown 2006-05-09	7.0	CVE-2006-2263 OTHER-REF FRSIRT SECUNIA BID
www.goel.ch -- 2005-Comments-Script	Multiple cross-site scripting (XSS) vulnerabilities in kommentar.php in 2005-Comments-Script allow remote attackers to inject arbitrary web script or HTML via the (1) id, (2) email, and (3) url parameter.	unknown 2006-05-09	7.0	CVE-2006-2290 OTHER-REF BID FRSIRT SECUNIA
X-Scripts -- X-Poll	X-Scripts X-Poll (xpoll) 2.30 allows remote attackers to execute arbitrary PHP code by using admin/images/add.php to upload a PHP file, then access it.	unknown 2006-05-09	7.0	CVE-2006-2281 BUGTRAQ MLIST BID FRSIRT SECUNIA

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
AngelineCMS -- AngelineCMS	SQL injection vulnerability in lib/adodb/server.php in AngelineCMS 0.6.5 and earlier might allow remote attackers to execute arbitrary SQL commands via the query string.	unknown 2006-05-11	4.7	CVE-2006-2328 BUGTRAQ OTHER-REF
AWStats -- AWStats	The web interface for AWStats 6.4 and 6.5, when statistics updates are enabled, allows remote attackers to execute arbitrary code via shell metacharacters in the migrate parameter.	unknown 2006-05-08	5.6	CVE-2006-2237 OTHER-REF OTHER-REF OTHER-REF BID FRSIRT OSVDB SECUNIA

Cisco -- Application Velocity System	The transparent proxy feature of the Cisco Application Velocity System (AVS) 3110 5.0 and 4.0 and earlier, and 3120 5.0.0 and earlier, has a default configuration that allows remote attackers to proxy arbitrary TCP connections, aka Bug ID CSCsd32143.	unknown 2006-05-11	4.7	CVE-2006-2322 CISCO BID FRSIRT
CutePHP -- CuteNews	CuteNews 1.4.1 allows remote attackers to obtain sensitive information via a direct request to (1) /inc/show.inc.php or (2) /inc/functions.inc.php, which reveal the path in an error message.	2006-05-05 2006-05-09	4.7	CVE-2006-2250 BUGTRAQ
Dokeos -- Open Source Learning & Knowledge Management Tool	PHP remote file inclusion vulnerability in authldap.php in Dokeos 1.6.4 allows remote attackers to execute arbitrary PHP code via a URL in the includePath parameter.	unknown 2006-05-09	5.6	CVE-2006-2285 BUGTRAQ BID FRSIRT SECUNIA BID
EQdkp -- EQdkp	PHP remote file inclusion vulnerability in includes/dbal.php in EQdkp 1.3.0 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the eqdkp_root_path parameter.	2006-05-08 2006-05-09	4.7	CVE-2006-2256 OTHER-REF BID FRSIRT SECUNIA
Evo-Dev -- evoTopsites Evo-Dev -- evoTopsites Pro	SQL injection vulnerability in index.php in evoTopsites 2.x and evoTopsites Pro 2.x allows remote attackers to execute arbitrary SQL commands via the (1) cat_id and (2) id parameters.	2006-05-08 2006-05-11	4.7	CVE-2006-2339 OTHER-REF BID FRSIRT SECTRACK SECUNIA
Expinion.net -- MultiCalendars	SQL injection vulnerability in all_calendars.asp in MultiCalendars 3.0 allows remote attackers to execute arbitrary SQL commands via the calsids parameter. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-05-09	4.7	CVE-2006-2293 BID SECUNIA
faktorystudios -- easyEvent	Cross-site scripting (XSS) vulnerability in index.php in easyEvent 1.2 allows remote attackers to inject arbitrary web script or HTML via the curr_year parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2006-05-08 2006-05-09	4.7	CVE-2006-2257 BID FRSIRT SECUNIA
FtrainSoft -- Fast Click	PHP remote file inclusion vulnerability in show.php in Fast Click SQL Lite 1.1.3 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the path parameter. NOTE: This is a different vulnerability than CVE-2006-2175.	2006-05-02 2006-05-09	4.7	CVE-2006-2241 BUGTRAQ OTHER-REF BID SECTRACK FRSIRT OSVDB SECUNIA XF
Inhouse Associates -- IA-Calendar	Cross-site scripting (XSS) vulnerability in calendar_new.asp in IA-Calendar allows remote attackers to inject arbitrary web script or HTML via the TypeName1 parameter. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-05-09	4.7	CVE-2006-2291 FRSIRT SECUNIA
Inhouse Associates -- IA-Calendar	Multiple SQL injection vulnerabilities in IA-Calendar allow remote attackers to execute arbitrary SQL commands via the (1) type parameter in (a) calendar_new.asp and (b) default.asp, and (2) ID parameter in (c) calendar_detail.asp. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-05-09	4.7	CVE-2006-2292 FRSIRT SECUNIA
Invision Power Services -- Invision Community Blog	SQL injection vulnerability in the do_mmod function in mod.php in Invision Community Blog (ICB) 1.1.2 final through 1.2 allows remote attackers with moderator privileges to execute arbitrary SQL commands via the selectedpids parameter.	2006-05-05 2006-05-09	4.7	CVE-2006-2251 BUGTRAQ BUGTRAQ OTHER-REF BID SECUNIA OSVDB
Jadu Limited -- Jadu CMS	Multiple cross-site scripting (XSS) vulnerabilities in Jadu CMS allow remote attackers to inject arbitrary web script or HTML via the (1) forename, (2) surname, (3) reg_email, (4) email_conf, (5) company, (6) city, (7) postcode, or (8) telephone parameters to site/scripts/register.php. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	2006-05-10 2006-05-11	4.7	CVE-2006-2305 FRSIRT SECUNIA
Jelsoft -- vBulletin	Jelsoft vBulletin accepts uploads of Cascading Style Sheets (CSS) and processes them in a way that allows remote authenticated administrators to gain shell access by uploading a CSS file that contains PHP code, then selecting the file via the style chooser, which causes the PHP code to be executed. NOTE: the vendor was unable to reproduce this issue in 3.5.x. NOTE: this issue might be due to direct static code injection.	2006-05-06 2006-05-11	4.2	CVE-2006-2335 BUGTRAQ OTHER-REF BUGTRAQ

Keyvan Janghorbani -- EPublisherPro	Cross-site scripting (XSS) vulnerability in moreinfo.asp in EPublisherPro allows remote attackers to inject arbitrary web script or HTML via the title parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2006-05-09 2006-05-11	4.9	CVE-2006-2306 BID FRSIRT SECUNIA
KeyVan1.com -- EDirectoryPro	SQL injection vulnerability in search_result.asp in EDirectoryPro 2.0 and earlier allows remote attackers to execute arbitrary SQL commands via the keyword parameter. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	unknown 2006-05-09	4.7	CVE-2006-2296 FRSIRT SECUNIA
Lethal Penguin -- PassMasterFlexPlus Lethal Penguin -- PassMasterFlex	Cross-site scripting (XSS) vulnerability in PassMasterFlex and PassMasterFlexPlus (PassMasterFlex+) 1.2 and earlier allows remote attackers to inject arbitrary web script or HTML via the (1) username, (2) password, or (3) User-Agent HTTP header in the Hack Log.	2006-05-04 2006-05-11	4.7	CVE-2006-2340 BUGTRAQ FRSIRT OSVDB SECUNIA XF
Mirabilis -- ICQ	Cross-Application Scripting (XAS) vulnerability in ICQ Client 5.04 build 2321 and earlier allows remote attackers to inject arbitrary web script from one application into another via a banner, which is processed in the My Computer zone using the Internet Explorer COM object.	2006-05-09 2006-05-11	4.7	CVE-2006-2303 BUGTRAQ SECTRACK
MyBulletinBoard -- MyBulletinBoard	Multiple SQL injection vulnerabilities in MyBB (aka MyBulletinBoard) 1.1.1 allow remote attackers to execute arbitrary SQL commands via the e-mail address when registering for a forum that requires e-mail verification, which is not properly handled in (1) usercp.php and (2) member.php.	2006-05-07 2006-05-11	4.7	CVE-2006-2333 BUGTRAQ OTHER-REF
MyBulletinBoard -- MyBulletinBoard	SQL injection vulnerability in showthread.php in MyBB (aka MyBulletinBoard) 1.1.1 allows remote attackers to execute arbitrary SQL commands via the comma parameter.	2006-05-09 2006-05-11	4.7	CVE-2006-2336 BUGTRAQ BID
MySQL -- MySQL	Buffer overflow in the open_table function in sql_base.cc in MySQL 5.0.x up to 5.0.20 might allow remote attackers to execute arbitrary code via crafted COM_TABLE_DUMP packets with invalid length values.	2006-04-25 2006-05-05	4.2	CVE-2006-1518 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF FRSIRT SECTRACK SECUNIA CERT-VN
Novell -- Novell client	Buffer overflow in DPRPCW32.DLL in Novell Client 4.83 SP3, 4.90 SP2 and 4.91 SP2 allows remote attackers to have an unknown impact via unknown attack vectors.	2006-05-10 2006-05-11	4.7	CVE-2006-2304 OTHER-REF FRSIRT SECUNIA BID SECTRACK
Novell -- Netware	Integer overflow in the DPRPCNLM.NLM NDPS/iPrint module in Novell Distributed Print Services in Novell NetWare 6.5 SP3, SP4, and SP5 allows remote attackers to have an unknown impact.	unknown 2006-05-11	4.7	CVE-2006-2327 OTHER-REF BID FRSIRT
Ocean12 Technologies -- Calendar Manager Pro	Multiple SQL injection vulnerabilities in Ocean12 Calendar Manager Pro 1.00 allow remote attackers to execute arbitrary SQL commands via the (1) date parameter to admin/main.asp, (2) SearchFor parameter to admin/view.asp, or (3) ID parameter to admin/edit.asp. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-05-09	4.2	CVE-2006-2264 BID FRSIRT SECUNIA
OpenFAQ -- OpenFAQ	Cross-site scripting vulnerability in submit.php in OpenFAQ 0.4.0 allows remote attackers to inject arbitrary web script or HTML via the q parameter.	2006-05-06 2006-05-09	4.7	CVE-2006-2252 BUGTRAQ BID FRSIRT SECUNIA
PHP-Fusion -- PHP-Fusion	PHP-Fusion 6.00.306 and earlier, running under Apache HTTP Server 1.3.27 and PHP 4.3.3, allows remote authenticated users to upload files of arbitrary types using a filename that contains two or more extensions that ends in an assumed-valid extension such as .gif, which bypasses the validation, as demonstrated by uploading then executing an avatar file that ends in ".php.gif" and contains PHP code in EXIF metadata.	2006-05-08 2006-05-11	4.7	CVE-2006-2330 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
PHP-Fusion -- PHP-Fusion	Multiple directory traversal vulnerabilities in PHP-Fusion 6.00.306 allow remote attackers to include and execute arbitrary local files via (1) a .. (dot dot) in the settings[locale] parameter in infusions/last_seen_users_panel/last_seen_users_panel.php, and (2) a .. (dot dot) in the localeset parameter in setup.php. NOTE: the vendor states that this issue might exist due to problems in third party local files.	2006-05-08 2006-05-11	4.7	CVE-2006-2331 BUGTRAQ OTHER-REF OTHER-REF BID FRSIRT SECUNIA

phpBB Group -- phpbb-auction	PHP remote file inclusion vulnerability in auction\auction_common.php in Auction mod 1.3m for phpBB allows remote attackers to execute arbitrary PHP code via a URL in the phpbb_root_path parameter.	2006-05-03 2006-05-09	4.7	CVE-2006-2245 OTHER-REF BID FRSIRT SECUNIA OSVDB XF
SmartISoft -- phpListPro	Multiple PHP remote file inclusion vulnerabilities in SmartISoft phpListPro 2.01 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the returnpath parameter in (1) editsite.php, (2) addsite.php, and (3) in.php. NOTE: The config.php vector is already covered by CVE-2006-1749.	2006-05-08 2006-05-11	5.6	CVE-2006-2323 BUGTRAQ BUGTRAQ
Tuomas Airaksinen -- Newsadmin	SQL injection vulnerability in readarticle.php in Newsadmin 1.1 allows remote attackers to execute arbitrary SQL commands via the nid parameter.	2006-05-04 2006-05-09	4.9	CVE-2006-2239 OTHER-REF FRSIRT SECUNIA BID OSVDB XF
Uapplication -- Ublog	Cross-site scripting (XSS) vulnerability in UBlog 1.6 Access Edition allows remote attackers to inject arbitrary web script or HTML via text fields when adding a blog entry.	2006-05-04 2006-05-09	4.7	CVE-2006-2246 OTHER-REF BID FRSIRT OSVDB SECUNIA
Vision Source -- Vision Source CMS	Multiple cross-site scripting (XSS) vulnerabilities in Vision Source 0.6 and earlier allow remote attackers to inject arbitrary web script or HTML via the fields in a user's profile.	unknown 2006-05-09	4.7	CVE-2006-2287 BUGTRAQ BID
Web4Future -- News Portal	Multiple cross-site scripting (XSS) vulnerabilities in Web4Future News Portal allow remote attackers to inject arbitrary web script or HTML via the ID parameter to (1) comentarii.php or (2) view.php. NOTE: this issue might be resultant from SQL injection.	2006-05-04 2006-05-09	4.7	CVE-2006-2243 SECTRACK OSVDB OSVDB SECUNIA
Web4Future -- News Portal	Multiple SQL injection vulnerabilities in Web4Future News Portal allow remote attackers to execute arbitrary SQL commands via the ID parameter to (1) comentarii.php or (2) view.php.	2006-05-04 2006-05-09	4.7	CVE-2006-2244 SECTRACK OSVDB OSVDB SECUNIA

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
3Com -- TippingPoint SMS Server	The web management interface in 3Com TippingPoint SMS Server before 2.2.1.4478 does not restrict access to certain directories, which might allow remote attackers to obtain potentially sensitive information such as configuration settings.	unknown 2006-05-09	2.3	CVE-2006-0993 BUGTRAQ OTHER-REF FRSIRT
acFTP -- acFTP	acFTP 1.4 allows remote attackers to cause a denial of service (application crash) via a long string with "{" (brace) characters to the USER command.	2006-05-05 2006-05-09	2.3	CVE-2006-2242 OTHER-REF BID FRSIRT OSVDB SECUNIA XF
AngelineCMS -- AngelineCMS	AngelineCMS 0.6.5 and earlier allow remote attackers to obtain sensitive information via a direct request for (1) adodb-access.inc.php, (2) adodb-ado.inc.php, (3) adodb-ado_access.inc, (4) adodb-ado_mssql.inc.php, (5) adodb-borland_ibase, (6) adodb-csv.inc.php, (7) adodb-db2.inc.php, (8) adodb-fbsql.inc.php, (9) adodb-firebird.inc.php, (10) adodb-ibase.inc.php, (11) adodb-informix.inc.php, (12) adodb-informix72.inc, (13) adodb-mssql.inc.php, (14) adodb-mssqlpo.inc.php, (15) adodb-mysql.inc.php, (16) adodb-mysqlt.inc.php, (17) adodb-oci8.inc.php, (18) adodb-oci805.inc.php, (19) adodb-oci8po.inc.php, and (20) adodb-odbc.inc.php, which reveal the path in various error messages; and via a direct request for the (21) lib/system/ directory and (22) possibly other lib/ directories, which provide a directory listing and "architecture view."	2006-05-07 2006-05-11	2.3	CVE-2006-2329 BUGTRAQ OTHER-REF

Apple -- Mac OS X	Multiple Apple Mac OS X 10.4 applications might allow context-dependent attackers to cause a denial of service (application crash) via a crafted EXR image file, which triggers the crash when opening a folder using Finder, displaying the image in Safari, or using Preview to open the file.	unknown 2006-05-09	2.3	CVE-2006-2277 BUGTRAQ
Arabless -- SaphpLesson	SaphpLesson 3.0 does not initialize array variables, which allows remote attackers to obtain the full path via an non-array (1) hrow parameter to (a) show.php or (b) index.php; the (2) Lsnrow parameter to (c) showcat.php; or the (3) rows parameter to index.php.	2006-05-04 2006-05-09	2.3	CVE-2006-2278 BUGTRAQ FRSIRT SECUNIA
Avahi -- Avahi	Avahi before 0.6.10 allows local users to cause a denial of service (mDNS/DNS-SD service disconnect) via unspecified mDNS name conflicts.	unknown 2006-05-09	3.3	CVE-2006-2288 OTHER-REF BID SECUNIA
Avahi -- Avahi	Buffer overflow in avahi-core in Avahi before 0.6.10 allows local users to execute arbitrary code via unknown vectors.	unknown 2006-05-09	1.6	CVE-2006-2289 OTHER-REF BID SECUNIA
CutePHP -- CuteNews	Multiple cross-site scripting (XSS) vulnerabilities in search.php in CuteNews 1.4.1 and earlier, and possibly 1.4.5, allow remote attackers to inject arbitrary web script or HTML via the (1) user, (2) story, or (3) title parameters.	2006-03-03 2006-05-09	2.3	CVE-2006-2249 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
D-Link -- DSL-G604T	Directory traversal vulnerability in webcm in the D-Link DSL-G604T Wireless ADSL Router Modem allows remote attackers to read arbitrary files via an absolute path in the getpage parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2006-05-07 2006-05-11	2.3	CVE-2006-2337 OTHER-REF SECTRACK
Drupal -- Drupal	Cross-site scripting (XSS) vulnerability in the project module (project.module) in Drupal 4.5 and 4.6 allows remote attackers to inject arbitrary web script or HTML via unknown attack vectors.	unknown 2006-05-09	2.3	CVE-2006-2260 OTHER-REF BID FRSIRT SECUNIA
Fujitsu -- NetShelter/FW-L Fujitsu -- NetShelter/FW-M Fujitsu -- NetShelter/FW-P Fujitsu -- NetShelter/FW	Unspecified vulnerability in the (1) web cache or (2) web proxy in Fujitsu NetShelter/FW allows remote attackers to cause a denial of service (device unresponsiveness) via certain DNS packets, as demonstrated by the OUSPG PROTOS DNS test suite.	2006-04-25 2006-05-09	2.3	CVE-2006-2240 OTHER-REF OTHER-REF BID SECUNIA
Ideal Science -- IdealBB	Unspecified vulnerability in Ideal Science Ideal BB 1.5.4a and earlier allows remote attackers to read arbitrary files under the web root via unspecified attack vectors related to the OpenTextFile method in Scripting.FileSystemObject.	unknown 2006-05-11	2.3	CVE-2006-2317 BUGTRAQ OTHER-REF BID
Ideal Science -- IdealBB	Incomplete blacklist vulnerability in Ideal Science Ideal BB 1.5.4a and earlier allows remote attackers to upload and execute an ASP script via a ".asa" file, which bypasses the check for the ".asp" extension but is executable on the server.	unknown 2006-05-11	3.3	CVE-2006-2318 BUGTRAQ IDEAL SCIENCE BID
Ideal Science -- IdealBB	Ideal Science Ideal BB 1.5.4a and earlier does not properly check file extensions before permitting an upload, which allows remote attackers to upload and execute an ASP script via a 0x00 character before the ".asp" portion of the filename.	unknown 2006-05-11	2.3	CVE-2006-2319 BUGTRAQ OTHER-REF BID
Ideal Science -- IdealBB	Multiple cross-site scripting (XSS) vulnerabilities in Ideal Science Ideal BB 1.5.4a and earlier allow remote attackers to inject arbitrary web script or HTML via unknown vectors. NOTE: due to lack of details from the researcher, it is not clear whether this overlaps CVE-2004-2207.	unknown 2006-05-11	2.3	CVE-2006-2321 BUGTRAQ OTHER-REF BID
Intel -- Intel PROset/Wireless	S24EvMon.exe in the Intel PROset/Wireless software, possibly 10.1.0.33, uses a S24EventManagerSharedMemory shared memory section with weak permissions, which allows local users to read or modify passwords or other data, or cause a denial of service.	2006-05-02 2006-05-11	2.3	CVE-2006-2316 BUGTRAQ REVERSE MODE BID FRSIRT
Internet Key Exchange -- Internet Key Exchange	The Internet Key Exchange version 1 (IKEv1) implementation in the libike library in Solaris 9 and 10 allows remote attackers to cause a denial of service (in.iked daemon crash) via crafted IKE packets, as demonstrated by the PROTOS ISAKMP Test Suite for IKEv1.	unknown 2006-05-10	2.3	CVE-2006-2298 OTHER-REF OTHER-REF SUNALERT BID FRSIRT SECTRACK SECUNIA

InterVations -- FileCOPA	Buffer overflow in filecpnt.exe in FileCOPA 1.01 allows remote attackers to cause a denial of service (application crash) via a username with a large number of newline characters.	unknown 2006-05-09	2.3	CVE-2006-2254 OTHER-REF FRSIRT SECUNIA BID
Kerio -- WinRoute Firewall	Kerio WinRoute Firewall before 6.2.1 allows remote attackers to cause a denial of service (application crash) via unknown vectors in the "email protocol inspectors," possibly (1) SMTP and (2) POP3.	unknown 2006-05-09	2.3	CVE-2006-2267 KERIO FRSIRT SECUNIA BID SECTRACK
Linux -- Linux Kernel	Memory leak in __setlease in fs/locks.c in Linux kernel before 2.6.16.16 allows attackers to cause a denial of service (memory consumption) via unspecified actions related to an "uninitialised return value," aka "slab leak."	2006-05-11 2006-05-11	1.6	CVE-2006-1859 OTHER-REF OTHER-REF FRSIRT SECUNIA
Linux -- Linux Kernel	lease_init in fs/locks.c in Linux kernel before 2.6.16.16 allows attackers to cause a denial of service (fcntl_setlease lockup) via actions that cause lease_init to free a lock that might not have been allocated on the stack.	2006-05-11 2006-05-11	1.6	CVE-2006-1860 OTHER-REF OTHER-REF OTHER-REF BID FRSIRT SECUNIA
Linux -- SCTP	Linux SCTP (lksctp) before 2.6.17 allows remote attackers to cause a denial of service (kernel panic) via incoming IP fragmented (1) COOKIE_ECHO and (2) HEARTBEAT SCTP control chunks.	unknown 2006-05-09	3.3	CVE-2006-2272 FULLDISC MU SECURITY OTHER-REF FRSIRT SECUNIA
Linux -- SCTP	Linux SCTP (lksctp) before 2.6.17 allows remote attackers to cause a denial of service (infinite recursion and crash) via a packet that contains two or more DATA fragments, which causes an skb pointer to refer back to itself when the full message is reassembled, leading to infinite recursion in the sctp_skb_pull function.	2006-05-06 2006-05-09	2.3	CVE-2006-2274 OTHER-REF
Linux -- SCTP	Linux SCTP (lksctp) before 2.6.17 allows remote attackers to cause a denial of service (deadlock) via a large number of small messages to a receiver application that cannot process the messages quickly enough, which leads to "spillover of the receive buffer."	unknown 2006-05-09	2.3	CVE-2006-2275 OTHER-REF
lksctp -- lksctp	The ECNE chunk handling in Linux SCTP (lksctp) before 2.6.17 allows remote attackers to cause a denial of service (kernel panic) via an unexpected chunk when the session is in CLOSED state.	unknown 2006-05-09	3.3	CVE-2006-2271 FULLDISC OTHER-REF OTHER-REF FRSIRT SECUNIA
MaxxCode -- MaxxSchedule	Cross-site scripting (XSS) vulnerability in Logon.asp in MaxxSchedule 1.0 allows remote attackers to inject arbitrary web script or HTML via the Error parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2006-05-08 2006-05-09	1.9	CVE-2006-2258 BID FRSIRT SECUNIA
Microsoft -- Windows NT Microsoft -- Windows 2000 Microsoft -- Windows Server 2003 Microsoft -- Microsoft Distributed Transaction Coordinator Microsoft -- Windows XP	Microsoft Distributed Transaction Coordinator (MSDTC) for Windows NT 4.0, 2000 SP4, XP SP1 and SP2, and Server 2003 allows remote attackers to cause a denial of service (crash) via a BuildContextW request with a large (1) UuidString or (2) GuidIn of a certain length, which causes an out-of-range memory access, aka the MSDTC Denial of Service Vulnerability. NOTE: this is a variant of CVE-2005-2119.	2005-10-11 2006-05-09	2.3	CVE-2006-1184 BUGTRAQ OTHER-REF MS BID FRSIRT SECUNIA
Microsoft -- Infotech Storage System Libary	Heap-based buffer overflow in Microsoft Infotech Storage System Library (itss.dll) allows user-complicit attackers to execute arbitrary code via a crafted CHM / ITS file that triggers the overflow while decompiling.	unknown 2006-05-09	3.7	CVE-2006-2297 BUGTRAQ BID
Microsoft -- Windows 2000 Microsoft -- Windows XP	The RtlDosPathNameToNtPathName_U API function in NTDLL.DLL in Microsoft Windows 2000 SP4 and XP SP2 does not properly convert DOS style paths with trailing spaces into NT style paths, which allows context-dependent attackers to create files that cannot be accessed through the expected DOS path or prevent access to other similarly named files in the same directory, which prevents those files from being detected or disinfected by certain anti-virus and anti-spyware software.	2006-05-09 2006-05-11	1.6	CVE-2006-2334 BUGTRAQ OTHER-REF BID
Mozilla -- Firefox	Mozilla Firefox 1.5.0.3 allows remote attackers to cause a denial of service via a web page with a large number of IMG elements in which the SRC attribute is a mailto URI. NOTE: another researcher found that the web page caused a temporary browser slowdown instead of a crash.	2006-05-06 2006-05-11	1.9	CVE-2006-2332 BUGTRAQ BUGTRAQ

myWebland -- MyBloggie	Cross-site scripting (XSS) vulnerability in myWebland MyBloggie 2.1.3 and earlier allows remote attackers to inject arbitrary web script or HTML via a JavaScript event in a BBCode img tag.	unknown 2006-05-09	2.3	CVE-2006-2269 BUGTRAQ BID
Northern Solutions -- Xeneo Web Server	Xeneo Web Server 2.2.22.0 allows remote attackers to obtain the source code of script files via crafted requests containing dot, space, and slash characters in the file extension.	2006-05-05 2006-05-09	2.3	CVE-2006-2248 OTHER-REF BID FRSIRT OSVDB SECUNIA
Ocean12 Technologies -- Calendar Manager Pro	Cross-site scripting vulnerability in admin/main.asp in Ocean12 Calendar Manager Pro 1.00 allows remote attackers to inject arbitrary web script or HTML via the date parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-05-09	1.9	CVE-2006-2265 BID FRSIRT SECUNIA
OnlyScript.info -- Online Universal Payment System Script	Directory traversal vulnerability in index.php in OnlyScript.info Online Universal Payment System Script allows remote attackers to read arbitrary files via directory traversal sequences in the read parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-05-11	2.3	CVE-2006-2326 BID FRSIRT SECUNIA
openEngine -- openEngine	Directory traversal vulnerability in website.php in openEngine 1.8 Beta 2 and earlier allows remote attackers to list arbitrary directories and read arbitrary files via a .. (dot dot) in the template parameter.	2006-05-07 2006-05-09	2.3	CVE-2006-2280 BUGTRAQ BID
PunBB -- PunBB	Cross-site scripting (XSS) vulnerability in misc.php in PunBB 1.2.11 allows remote attackers to inject arbitrary web script or HTML via the req_message parameter, because the value of the redirect_url parameter is not sanitized.	unknown 2006-05-05	2.3	CVE-2006-2227 BUGTRAQ SECUNIA BID FRSIRT
Quagga -- Quagga Routing Software Suite	bgpd in Quagga 0.98 and 0.99 before 20060504 allows local users to cause a denial of service (CPU consumption) via a certain sh ip bgp command entered in the telnet interface.	2006-03-28 2006-05-09	2.3	CVE-2006-2276 MLIST OTHER-REF OSVDB
Roger Aelbrecht -- TZipBuilder	Buffer overflow in TZipBuilder 1.79.03.01 allows remote attackers to execute arbitrary code via a ZIP archive that contains a file with a long file name.	2006-05-08 2006-05-09	2.3	CVE-2006-2161 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
singapore -- singapore	Cross-site scripting (XSS) vulnerability in index.php in singapore 0.9.7 allows remote attackers to inject arbitrary web script or HTML via the image parameter.	unknown 2006-05-09	1.9	CVE-2006-2262 BUGTRAQ OTHER-REF BID
Symantec -- Enterprise Firewall Symantec -- Gateway Security	The HTTP proxy in Symantec Gateway Security 5000 Series 2.0.1 and 3.0, and Enterprise Firewall 8.0, when NAT is being used, allows remote attackers to determine internal IP addresses by using certain HTTP requests.	unknown 2006-05-11	2.3	CVE-2006-2341 OTHER-REF BID FRSIRT SECTRACK SECTRACK SECUNIA
TDC -- Cryptomathic Cenroll ActiveX Control	Stack-based buffer overflow in the createPKCS10 function in Cryptomathic Cenroll ActiveX Control 1.1.0.0 allows remote attackers to execute arbitrary code via vectors related to the TDC Digital signature.	2006-05-05 2006-05-09	2.3	CVE-2006-1172 BUGTRAQ OTHER-REF BID FRSIRT OSVDB SECTRACK SECUNIA
VeriSign -- i-Nav	The InstallProduct routine in the Verisign VUpdater.Install (aka i-Nav) ActiveX control does not verify Microsoft Cabinet (.CAB) files, which allows remote attackers to run an arbitrary executable file.	2006-03-27 2006-05-11	2.3	CVE-2006-2273 BUGTRAQ OTHER-REF BID FRSIRT
WebCalendar -- WebCalendar	WebCalendar 1.0.1 to 1.0.3 generates different error messages depending on whether or not a username is valid, which allows remote attackers to enumerate valid usernames.	2006-05-04 2006-05-09	2.3	CVE-2006-2247 BUGTRAQ BUGTRAQ BID SECUNIA OSVDB

Website Baker -- Website Baker	Cross-site scripting (XSS) vulnerability in Website Baker CMS allows remote attackers to inject arbitrary web script or HTML via a user display name.	unknown 2006-05-11	2.3	CVE-2006-2307 BUGTRAQ BID XF
X7 Group -- X7 Chat	Cross-site scripting (XSS) vulnerability in X7 Chat 2.0.2 and earlier allows remote attackers to inject arbitrary web script or HTML via a javascript URI in the URL of an avatar, possibly related to the avatar parameter in register.php.	2006-04-06 2006-05-09	2.3	CVE-2006-2282 BUGTRAQ BID FRSIRT OSVDB SECUNIA

Back to top

Last updated May 15, 2006